Unisys

Digital Signature

Slide 1 of 35

This presentation..

- What is “Universal Access”
  - Traditional considerations
  - Impact of changing requirements
- Authentication
  - Identify - verify
- Trust relationships
- Role of the Government

Towards Universal access

Traditional Considerations

- Single Sign-On
  - Identify once - gain access to several systems
  - Userid Password - many to one mapping
- Password synchronization
- Centralized Security Administration
  - Target systems still maintained the name space

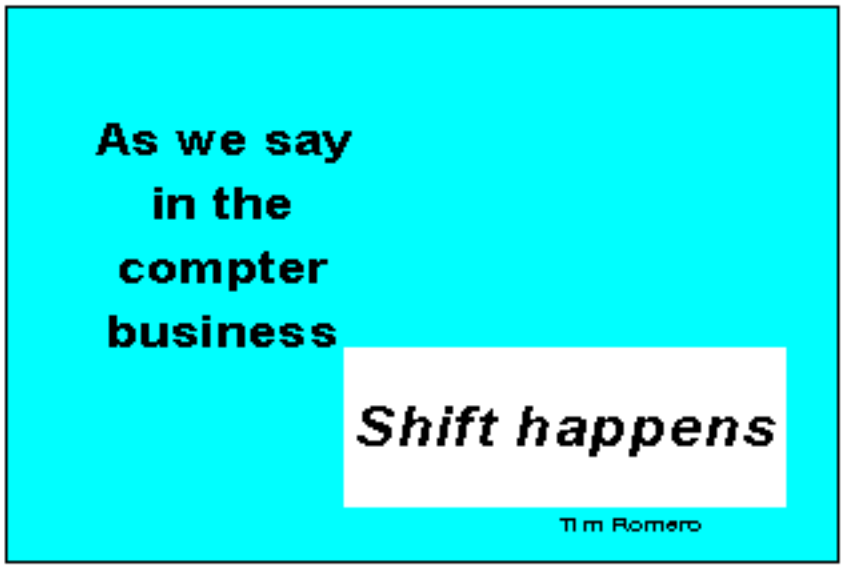
Unisys

3

Slide 3 of 35

Towards Universal access

Shifting paradigm

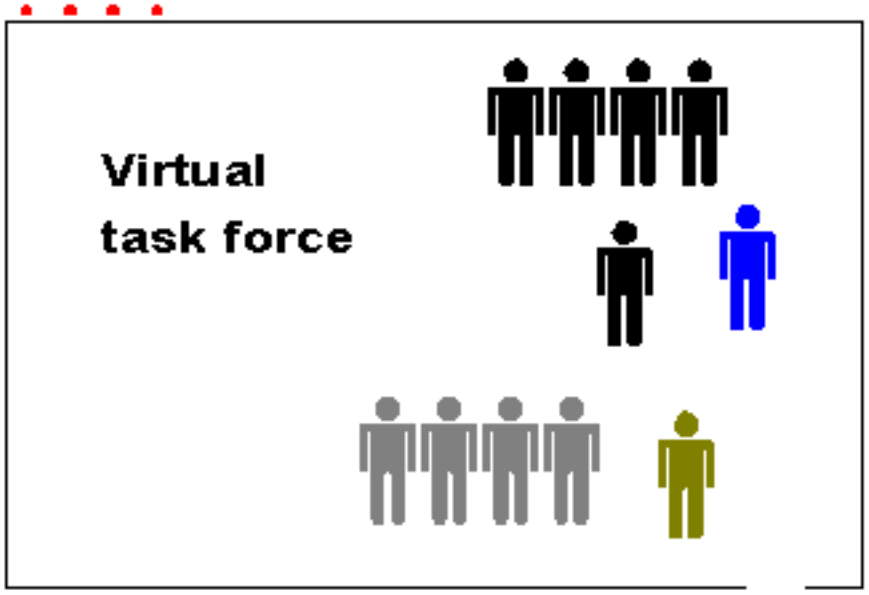


Unisys

Slide 4 of 35

Towards Universal access

- Changing Personnel requirements



Unisys

Slide 5 of 35

Towards Universal access
- Changing Technology

- cable TV, Long Distance common carriers, regional RBOCs
- Computers, telephones, news, FAX...
- Video on demand, databases, homeshopping, bill paying,banking ....
- Interacting Devices - VCRs, Digital Cameras, PDAs..
  - Jini, M/S Cool, Bluetooth
- Security
  - Internet
  - Web
  - Language ...
  - Authentication of end entities

The issues

- Is it legal?
  - Is the transaction legal
  - properly signed
  - the intent of transaction
  - transacting parties
- Trusting the message without out-of-band verification
  - message not altered
  - who sent the message
- The chain of trust
  - Evolution of the certificate
  - CA policies and practices

Government's role

- E-commerce legislation/regulations
  - Taxation of e-commerce transactions
  - Jurisdiction over on-line transactions
  - **data protection and privacy**
  - **Confidentiality of e-commerce transactions**
  - information security
  - **enforceability of e-commerce transactions**
- Promote or Control

Government's role
data protection and privacy

- **Databases**
  - Collection, use, and dissemination of information
  - protection
- **Collection by**
  - asking questions
  - by placing "Cookies" and other means
- **Use**
  - Legal - any implications? - unintended usage
- **Dissemination**
  - shared with or sold to undisclosed third parties - legal issues
- **Protection**
  - from unauthorized access or disclosure by employees, hackers, or others
  - information provider's consent is valid and legally binding
  - not being obtained from children

enforceability of e-commerce transactions - electronic Signature legislation

- America Bar Association Digital Signature Guidelines
  - Utah Digital Signature Act '95
  - Technology specific
- California
  - Technology neutral
- US Federal Government, 49 states, over 15 countries,
- National Conference of Commissioners of Uniform State Laws -
  - Uniform Electronic Transactions Act (UETA).
- European Union
- United Nations Commission on International Trade Laws (UNCITRAL)
  - Model Law on Electronic Commerce
  - International legislation -
    - digital Signature
    - Certification Authority

Unisys

10

Slide 10 of 35

Establishment of TRUST & PREDICTABILITY in e-commerce

- Remove barriers, and promote the establishment of "Trust" and "Predictability" required by parties doing business on-line
- Legislation so far....
  - minimalist approach - use of electronic signatures in limited circumstances to
  - Very formal, highly regulatory approach governing the manner in which digital signatures can be used and Certification Authorities may operate
- the legislative approaches to to removing barriers to e-commerce have been varied and inconsistent, and may have actually made the situation worse

Unisys

11

Slide 11 of 35

Typical authentication tokens

- Finger: fingerprint & geometry
- Signature
- Hand: geometry, vein & palm
- Eye: iris & retina
- Facial: standard & thermal
- Voice
- Others

Slide 12 of 35

Signing an electronic record

- Name typed at the end of a e-mail message
- Digitized image of handwritten signature attached (Signature dynamics)
- Finger print image
- Finger print minutiae
- a handle - PIN

- "*Digital signature*" - a term for one technology-specific type of electronic signature. It involves the use of public key cryptography to "sign" a message

Symbol that signifies intent..

- Signature
  - Intention to authenticate a writing
- Digital signature in addition to above
  - Identifies the person signing
  - evidence of the integrity of document
- Government's view for the states

"and that such a foundation should be based upon a simple, technology neutral, non-regulatory, and market-based approach."

UNCITRAL Model Law

- an electronic signature must include a method to identify the signer
- an electronic signature must include a method to indicate the signer's approval of the information contained in the message
- the method used must be as reliable as was appropriate for the purpose for which the message was generated or communicated

California - qualification

- California
  - unique to the person using it
  - capable of verification
  - under the sole control of the person using it
  - linked to the data in such a manner that if the data is changed, the signature is invalidated.

Digital Signature....mostly

- Utah
- Washington
- Minnesota
- Missouri
- New Hampshire

Slide 17 of 35

State of Virginia

VIRGINIA

- unique to the signer
- capable of verification
- under the signer's sole control
- linked to the record in such a manner that it can be determined if any data contained in the record was changed subsequent to the electronic signature being affixed to the record
- created by a method appropriately reliable for the purpose for which the electronic signature was used.

Unisys

18

Slide 18 of 35

Authorized types of transactions varies..

- 40% of states - all transactions
- UCC filings, medical records, motor vehicle records
- More specific to parties involved in the transaction
  - Between government agencies
  - Between Government agency and other

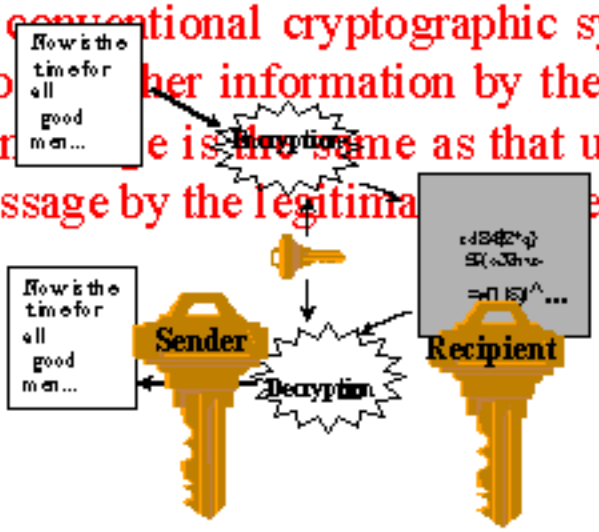
Fundamentals...

- Symmetric Keys
- Asymmetric Keys
- Hash Functions
- Digital Signature
- Certificates

Fundamentals... Symmetric Keys

…DES,IDEA,GOST,CAST,BLOWFISH…...

- In the conventional cryptographic systems, the key used to [illegible]her information by the originator of a secret m[illegible]e is the same as that used to decipher the message by the legitima[illegible]ent.



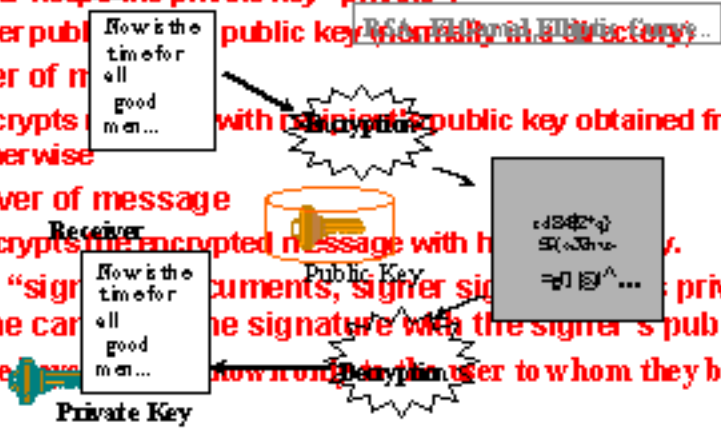
Unisys

21

Slide 21 of 35

Fundamentals... Asymmetric Keys

- Keys come in pairs - Private & Public
  - Messages encrypted by one key can only be decrypted by the other.
  - User keeps the private key "private".
  - User publishes public key (normally in a directory)
- Sender of message
  - encrypts message with recipient's public key obtained from directory or otherwise
- Receiver of message
  - decrypts the encrypted message with his private key.
- When "signing" documents, signer signs with his private key and anyone can verify the signature with the signer's public key.
- Private keys must be known only by the user to whom they belong

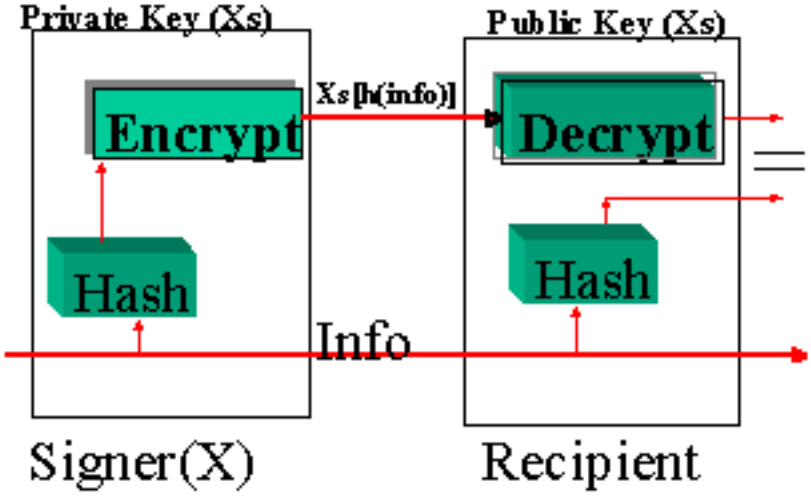


Hash Functions

- Has many names
  - compression function, contraction function,message digest,fingerprint, cryptographic checksum,message integrity check (MIC), Manipulation Detection Code (MDC).
- The hash function shall be one-way
- The hash function shall be collision-free
- A function which maps values from a large domain into a smaller range.

Unisys

Digital Signature.

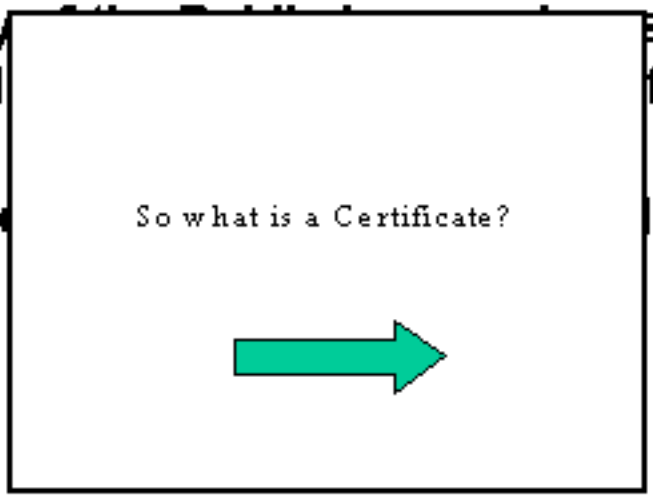


Signs Information (info) by appending to the info an
The signed information includes the hashing algorithm and the
encryption algorithm used to compute the digital signature.

Unisys

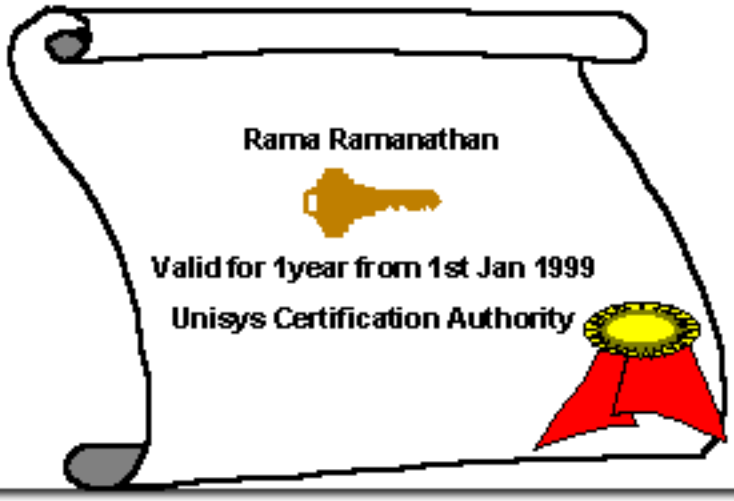
So why a certificate?

- Validity [illegible] scertained regardl [illegible] formation from
- helps t [illegible] less secure



Fundamentals... Certificates

- The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.



Unisys

26

Slide 26 of 35

Information in the certificate..

Version .....of the certificate

Serial Number.....of the certificate

Signature..... algorithm used to sign the certificate

Issuer.....name of the CA which signed this certificate

Validity.....the first and last on which the certificate is valid

Subject .....The distinguished name of the owner

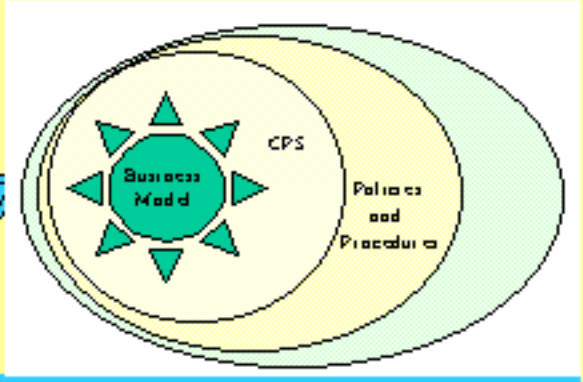
subjectPublicKeyInfo.....The Algorithm and the users's public key

issuerUniqueIdentifier ..... To further identify the CA

subjectUniqueIdentifier.....To further identify the user

Extensions .....a method of putting more info without destroying base.

Who makes the Certificates?



- CERTIFICATION AUTHORITY

Unisys

28

Slide 28 of 35

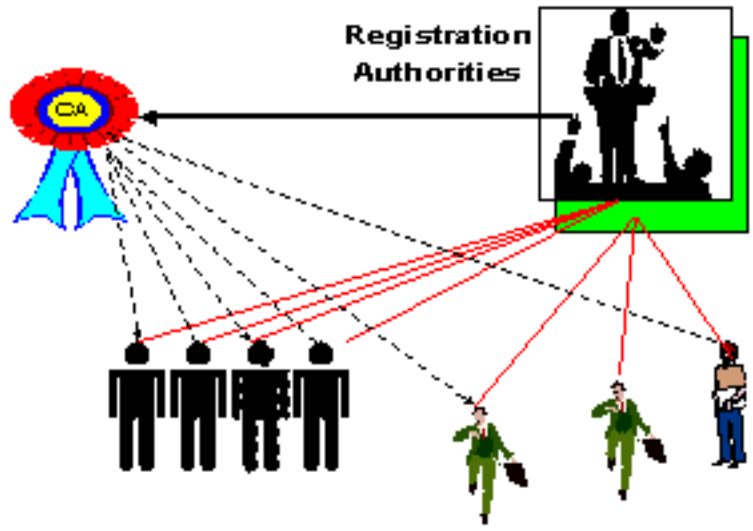
Duties of a CA

- **OBLIGATION:**
  - To subscribers
  - Parties relying on the Certificates, CRLs and repositories maintained by CA
  - Third party victims of fraud
- **Policy**
- **Certificate Practice Statement (CPS)**
- **"Say what you do.. And do what you say"**
- **Must be auditable**

Various points of trusts

- Embedded CA s
- Enterprise CAs
- National CA s
- Industry level CA s
- International CA s

The question of trust

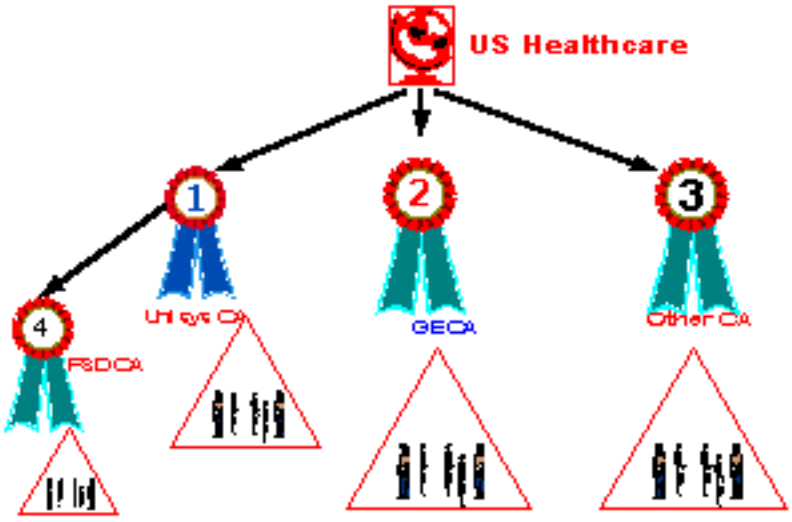


Unisys

31

Slide 31 of 35

Establishing "Signing (CA) Hierarchies"
The Hierarchical model



Unisys

32

Slide 32 of 35

Establishing "Signing Hierarchies"
The "Trust Models"

- hierarchical model
- a web of trust model
- A Cross-authenticated model - extranets

The Certificate Authority

- Establish “Signing Hierarchies”
- Promulgate Certificate policy and CPS
- Accept and review applications
- Name Subscribers
- Issue Certificates
- Revoke and suspend Certificates
- Maintain Repository
- Publish certificates and CRLs
- Provide ancillary services

Unisys

34

Slide 34 of 35

Questions

Slide 35 of 35